#12
KWS
6-21-01

In the United States Patent and Trademark Office

Serial Number: 09/081,872
Appn. Filed: 05/20/98
Applicant(s): John H. Messing
Appn. Title: Electronic Signature Program
Examiner: Douglas J. Meislahn
Group Art Unit: 2767

Mailed: June 12, 2001

At: Tucson, Arizona

Declaration Under Rule 132

JOHN H. MESSING, declares as follows:

1. I am the inventor in Serial Number 09/081,872. Originally, I was a practicing trial lawyer, which I did for many years. Then I began to write and develop software for one of the first Internet court filing projects in my hometown, which is Tucson, Arizona. It involved a small claims court, which while humble, allows ordinary citizens to resolve claims that otherwise might go unheard, and helps to lessen the possibility of violence to settle disputes. With the Internet, people can file from home or work and avoid a long drive downtown and wait in line simply to file a piece of paper and pay a fee.
2. It seemed natural that the filings would need a signature. I became an active member of the American Bar Association's Information Security Committee, which studies and develops standards for electronic signatures and published the Digital Signature Guidelines. I attempted to use a Public Key Infrastructure for the small claims project. I worked extensively with PKI. I became a beta tester for Entrust's first software offering, which was called WebCA and which was released in 1997. I was featured in the product's press release, which is still available on the

www.entrust.com website, as a knowledgeable source who could attest to its usefulness. The product itself was very good, but the court officials found it too difficult for people to use practically and too expensive over the long term. I was asked to invent "something else." I came up with this invention.

3. At the time I filed the patent application in 1998, the idea of using a server to sign on behalf of people and verify their signatures was thought to be heretical. But it is effective, much less expensive than a PKI, and after almost 700 court filings without mishap, has gained acceptance. For that project I used asymmetric encryption only.
4. The Court project received recognition. It became the subject of a law review article which I helped to write entitled "Electronic Court Filing in The Pima County Small Claims Court -- Technical Parameters, Adopted Solutions, and Some of the Legal Issues Involved", 38 Jurimetrics J. 397-406 (1998)(American Bar Association) and the Justice Court was named one of the top ten court websites in the Spring of 2000, see http://www.justiceserved.com, in large part because of the benefits of the signature invention.
5. The court has paid me for the efiling project with its signature technology for public filings since May, 1998. Recently (May, 2001) I was awarded a second contract by the Arizona Court of Appeals, for the asymmetric version of this signature technology (and not for efiling as such) for use in filings of briefs, notices, motions and orders. The Court of Appeals is the second highest court in the State of Arizona. I make it a practice to keep up with developments in this field. The announced use of electronic signatures using the technology of this invention by the Arizona Court of Appeals for appeals of various kinds, including civil and criminal briefs is one of the first steps ever taken by any court in any country to make use of an electronic signature technology for general court usage.

6. I have been requested and agreed to act as a paid consultant to a grouping of law enforcement agencies in the Phoenix area on electronic signature issues. The desirability of the technology of this invention, as opposed to digital signatures generated with digital certificates of client side users or others discussed in the specification, as conveyed to me by the various staff people involved at the courts and the law enforcement agencies, has been based upon one or more of the following advantages of the invention: ease of use, convenience, ability to utilize ordinary database information about users for signature and verification purposes, minimal impact upon historic workflows, lack of interoperability issues, reduced cost, and performance.
7. In 1999, I became the co-chair of the Signatures Workgroup of LegalXML, which deals with electronic signature of XML documents and document fragments using document tags, in connection with legal documents and court filings. Recently, I became a participating contributor and member of the W3C Encryption Workgroup which deals with encryption of XML documents and document fragments using document tags. I remain a member of the ABA's Information Security Committee. As part of my involvement with standards bodies I have been made aware of the efforts of the digital signature workgroup of the W3C, to which I do not belong, to create digital signatures with tagged documents using XML, which is the principal body recognized internationally as involved in this effort. See http://www.w3.org/TR/2001/CR-xmldsig-core-20010419/, which is the April 2001 latest candidate recommendation of the digital signature workgroup of the W3C. Various interoperability issues regarding X-509 certificate information retrieval have been reported in the laboratory trials of the work product of the group. I have discovered over the years that interoperability issues commonly occur in electronic signature solutions that depend upon client side digital certificates issued pursuant to

a PKI. I have concluded from the experience of this workgroup that use of tags with digital signatures is not old and accepted, contrary to what was stated by official notice in the office action which was mailed March 13, 2001, but on the contrary is new, ongoing and unfinished, and that prior art based upon client side digital certificates suffers from certain chronic and perhaps insoluble interoperability issues.

8. Since the filing of this application and parallel to the acceptance of the invention by the several courts, a change has occurred in the PKI industry. Times have become very tough. Brilliant people are being laid off from major companies. The technology is becoming known as difficult, expensive, and to be avoided. Recently, with a public announcement in February 2001 in Cambridge, Mass. at a meeting of the W3C, an initiative was launched by VeriSign, Microsoft and others to examine the use of servers with PKI, which is called XKMS, as a protocol for XML-based key management, and which does not necessarily require client-side certificates to be used to establish signature trust. The public website online at this time for the initiative is http://www.xkms.org. There is an understanding that server authentication is being recommended in place of client side keys and PKI. That development follows the lead of this invention, and is obtaining adherents. What just a few years ago was once considered so unorthodox as to constitute heresy is now being considered practical and perhaps inevitable. In 1998, the invention was very novel. Today it is gaining acceptance.

9. It is not true, as the office action mailed March 13, 2001 asserts as a matter of official notice that MACs have been widely used to create signatures. As the Ford and Baum book "Secure Electronic Commerce" at p. 320 (attached to the amended form 1449) states and I agree with the statement, MAC's logically cannot be used for non-repudiable signatures where the originator and recipient each have a copy of the symmetric key because a neutral judge cannot tell which party applied the

encryption. It is a classic problem. The problem is solvable with this invention. Where a single server alone holds the key and signs and verifies for others, then only it could have applied the key. That is a novel and unexpected result of the business method patent sought.

10. A fundamental difference between this invention and the prior art described by Ford and Baum is that in this invention the server does both the signing and verifying on the basis of its knowledge of the signers and possession of the keys while in Ford and Baum, the trusted third party only does the signing, while the recipients each verifies the signature using the public key of the trusted third party.

11. This invention also allows for many types of knowledge about signers to be used in determining signature privileges, depending on the importance, value and sensitivity of the information to be signed and the requirements of the verifying party. A small claims complaint is not very valuable or sensitive and a simple credit card approval by a credit card company may be enough to authenticate the signer. But other documents may require higher authentication levels. For example, an order in an important appellate case may require the judge to enter both a password and provide a biometric identifier before the source will be trusted by another court. With a single server, both the small claims complaint and the appellate order can be signed and verified with different authentication means using the same system. In Ford and Baum's model of a trusted third party signer, where the trusted third party does only the signing but not the verifying, the authentication mechanism is far less flexible. The only types of authentication that are allowable according to Baum and Ford are public keys with digital certificates and Kerberos tokens. Ford and Baum are talking about something very different from this business method invention and their book did not describe this invention or even suggest it.

I hereby declare that all statements made herein are true or are made on information or belief and are believed to be true; and further that these statements were made with the knowledge that willfully false statements so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Dated: June 11, 2001

John H. Messing
Inventor